

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all previous versions and listings of claims in this application.

Claim Listing:

Claims 1-19: (Canceled).

20. (Currently Amended) A security module suitable for use with a digital currency depot for producing a forgery-proof document, the module comprising:

an identification register, a key register and a secret generator that generates an unpredictable secret;

a first combination machine ~~that combines~~ arranged to combine an output value of the identification register and an output value of the secret generator;

an encryption machine ~~that encrypts~~ arranged to encrypt an output value of the first combination machine to an authentication unit via a first outlet valve;

~~a first outlet valve that outputs an encrypted output of the encryption machine via an authentication unit;~~

a second combination machine that combines the unpredictable secret and input data received via an inlet valve;

a hash machine that generates and outputs an irreversible hash value responsive to an output of the second combination machine; and

~~a second outlet valve that outputs the hash value;~~

~~wherein the hash value is independent of contents of the forgery-proof document~~
means for ensuring that the forgery-proof document is produced only if actual sums of money are available to the digital currency depot.

21. (Previously presented) The security module of claim 20, further comprising a key register coupled to the encryption machine, wherein at least one value stored in the key register is used by the encryption machine to provide the encrypted output of the first combination machine.

22. (Currently amended) A method for producing a forgery-proof document, the method comprising:

using the security module of ~~claim 18; and claim 20;~~
~~outputting the hash value from the second outlet valve~~
providing the output of the second combination machine as forgery-proof information to the forgery-proof document; and
issuing the forgery-proof document.

23. (Currently amended) A method for producing a forgery-proof document, the method comprising:

generating an unpredictable secret;

combining an output of an identification register and the unpredictable secret;
encrypting the combined output of the identification register and the unpredictable secret;
outputting the encrypted combined output to an authentication unit;
combining the secret and the input data input via an inlet valve;
using the combined secret and input data to form an irreversible hash value; ~~and~~
~~outputting the hash value;~~
~~wherein the hash value is independent of contents of the forgery-proof document~~
interfacing with a digital currency depot; and
ensuring that only sums of money actually available to the digital currency depot are used
to produce the forgery-proof document.

24. (Currently amended) The method of claim 23, wherein said outputting comprises
outputting the irreversible hash value to the forgery-proof document as forgery-proof
information.

Claims 25-27: (Canceled).

28. (New) The security module of claim 20, wherein the irreversible hash value is
output as forgery-proof information to the forgery-proof document.

29. (New) The security module of claim 20, further comprising means for reducing a register value associated with a particular currency sum available to the digital currency depot in response to production of the forgery-proof document.

30. (New) A system for effectuating payments for services involving forgery-proof documents, the system comprising:

a digital currency depot;

a security module operatively connected to the digital currency depot for producing the forgery-proof documents, wherein the security module comprises:

an identification register, a key register and a secret generator that generates an unpredictable secret;

a first combination machine arranged to combine an output value of the identification register and an output value of the secret generator;

an encryption machine arranged to encrypt an output value of the first combination machine to an authentication unit via a first outlet valve;

a second combination machine that combines the unpredictable secret and input data received via an inlet valve;

a hash machine that generates and outputs an irreversible hash value responsive to an output of the second combination machine; and

means for ensuring that a forgery-proof document is produced only if actual sums of

money are available for use by the digital currency depot.

31. (New) The system of claim 30, wherein the forgery proof document is produced as a postage stamp.

32. (New) The system of claim 30, wherein the security module further comprises a storage device that stores information relating to a currency and a sum that can currently be used to produce the forgery proof document.

33. (New) The system of claim 30, wherein the security module further comprises a storage device that stores information relating to a currency and a total sum that has been expended to produce forgery proof documents.